(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 518 315 B1

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
10.09.1997 Bulletin 1997/37

(51) Int Cl.[6]: **H04L 9/06**

(21) Application number: **92109814.1**

(22) Date of filing: **11.06.1992**

(54) **System and method for blockwise encryption of data**

Einrichtung und Verfahren zum blockweisen Verschlüsseln von Daten

Dispositif et procédé de chiffrage de données par blocs

(84) Designated Contracting States:
DE FR GB NL

(30) Priority: **13.06.1991 JP 141911/91**

(43) Date of publication of application:
16.12.1992 Bulletin 1992/51

(73) Proprietor: **MITSUBISHI DENKI KABUSHIKI KAISHA**
Chiyoda-ku Tokyo (JP)

(72) Inventor: **Matsui, Mitsuru,**
c/o Mitsubishi Denki K.K.
Kamakura-shi, Kanagawa (JP)

(74) Representative: **Pfenning, Meinig & Partner**
Mozartstrasse 17
80336 München (DE)

(56) References cited:
EP-A- 0 406 457

- **ICC'81, DENVER vol. 2(4), June 1981, IEEE, NY,USA pages 40.1.1 - 40.1.15 BANERJEE 'Million Bits of DES Encryption in the Blink of an Eye'**

EP 0 518 315 B1

Printed by Jouve, 75001 PARIS (FR)

Description

BACKGROUND OF THE INVENTION

i) Field of the Invention:

The present invention relates to data communication system and method with a data scrambling, and more particularly to an improvement of data communication system and method which perform a digital data array configuration change according to a certain scramble function to carry out a secret communication.

ii) Description of the Related Arts:

Conventionally, a wireless transmission or a transference of various data is carried out for processing the data, it is sometimes necessary to substantially conceal such data.

In such a case, for example, it is useful to prevent a tapping of conversation data in a radio telephone communication, and it is preferable to perform a certain kind of modulation of the conversation data in order not to be understood by an interceptor even when the conversation data to be transmitted by an electric wave are intercepted.

Also, when an ID number of a cash card of a bank or the like can be readily read out by the third party, the safety of the cash card can not be held, and in such a case, it is also preferable to prevent an analysis or decoding of the card data without using a particular read key or password.

Further, in the near future, the spread of an IC card is realized and in certain cases, an ID number for a bank account is written or much other private information considered to be secret is recorded in the card. In order to prevent the ready reading of the private information from the IC card, it is preferable to record the data in the card after the above-described modulation of the data contents.

Accordingly, at the data communication or transference, it is desired to perform the radio or data communication or data recording is performed while the data are made secret as described above.

In the data modulation of this kind, in case of digital data to be handled, the modulated data can be relatively readily made secret, and a simplest and most effective modulation is known as a data scrambling. A principle of a conventional system capable of applying to this scramble modulation will be described hereinbelow.

In Fig. 5, there is shown a data scrambling system using the principle of a conventional data encryption system, for example, a FEAL-8 cipher algorithm, as disclosed in "Fast Data Encipherment Algorithm FEAL-8" by Miyaguchi, Shiraishi and Shimizu, NTT Research Practicing Report, Volume 37, Nos. 4 to 5, 1988. In the drawing, numerals 13 and 14 denote an 8 bytes of plaintext and an 8 bytes of scrambled text, respectively, and the data scrambling system includes a plurality of processing blocks (PBs) 15, 16, 17 and 18 for converting an input signal by using a part of extended keys as a parameter to output a converted signal, a plurality of exclusive logical ORs 21 and an magnification key latch 22 for storing 32 bytes of extended keys.

Next, the operation of the data scrambling system shown in Fig. 5 will now be described. First, an exclusive OR of the input plaintext 13 and the 8 bytes from the 0 byte to the 7 byte of the extended key output from the extended key latch 22 is calculated, and then the exclusive OR of the insignificant 4 bytes and the significant 4 bytes of the calculation result is calculated to output the calculation result to the next step.

Then, the insignificant 4 bytes of the previous step output are input to the processing block 15 and the processing block 15 converts the input signal by using the two bytes from the 8 byte to the 9 byte of the magnification key output from the extended key latch 22 as a parameter to output a converted signal. The exclusive OR of the output of the processing block 15 and the significant 4 bytes of the previous step output is calculated, and the significant 4 bytes and the insignificant 4 bytes of the calculation result are replaced with each other to output the obtained signal to the next step.

Next, the insignificant 4 bytes of the previous step output is input to the processing block 16 and the processing block 16 converts the input signal by using the two bytes from the 10 byte to the 11 byte of the magnification key output from the extended key latch 22 as the parameter to output a converted signal. The exclusive OR of the output of the processing block 16 and the significant 4 bytes of the previous step output is calculated, and the significant 4 bytes and the insignificant 4 bytes of the calculation result are replaced with each other to output the obtained signal to the next step.

Then, the same operation as described above is repeated eight times to the processing block 18. Next, after the significant 4 bytes and the insignificant 4 bytes of the calculation result are replaced with each other, the exclusive OR of the significant 4 bytes and the insignificant 4 bytes is calculated. Further, the exclusive OR of the calculation result and the 8 bytes from the 24 byte to the 31 byte of the extended key output from the extended key latch 22 is calculated to output the scrambled text 14.

In Fig. 6, there is shown a data scrambling system using the principle of another conventional data encryption system, for example, a MULTI-2 cipher algorithm, as disclosed in "Multi-Media Encryption Algorithm", by Takaragi, Sasaki and Nakagawa, Multimedia Communication and Dispersed Processing, 40-5, 1989. In the drawing, numerals 13 and 14 denote a 64 bits of plaintext and a 64 bits of scrambled text, respectively, and the data scrambling system has the same construction as the above-described data scrambling system shown in Fig. 5 except processing blocks (PBs) 15, 16, 17, 18, 19 and 20.

Next, the operation of the data scrambling system shown in Fig. 6 will now be described. First, the input plaintext 13 is divided into significant 32 bits and insignificant 32 bits, and the exclusive OR of the significant 32 bits and the insignificant 4 bits is calculated to output a first calculation result to the processing block 15. The processing block 15 converts the input signal by using the 32 bits from the 0 bit to the 31 bit of the extended key output from the extended key latch 22 as the parameter to output a converted signal. The exclusive OR of the output of the processing block 15 and the significant 32 bits is calculated to output a second calculation result to the processing block 16, and the processing block 16 converts the input signal by using the 64 bits from the 32 bit to the 95 bit of the extended key output from the extended key latch 22 as the parameter to output a converted signal. The exclusive OR of the output of the processing block 16 and the first calculation result of the above-described exclusive OR is calculated to output a third calculation result to the processing block 17, and the processing block 17 converts the input signal by using the 32 bits from the 96 bit to the 127 bit of the extended key output from the extended key latch 22 as the parameter to output a converted signal. The exclusive OR of the output of the processing block 17 and the second calculation result of the above-described exclusive OR is calculated to output a fourth calculation result.

Then, the exclusive OR of the third and fourth calculation results of the above-described exclusive ORs is calculated to output a fifth calculation result to the processing block 18, and the processing block 18 converts the input signal by using the 32 bits from the 128 bit to the 159 bit of the extended key output from the extended key latch 22 as the parameter to output a converted signal. The exclusive OR of the output of the processing block 18 and the fourth calculation result of the above-described exclusive OR is calculated to output a sixth calculation result to the processing block 19, and the processing block 19 converts the input signal by using the 64 bits from the 160 bit to the 223 bit of the extended key output from the extended key latch 22 as the parameter to output a converted signal. The exclusive OR of the output of the processing block 19 and the sixth calculation result of the above-described exclusive OR is calculated to output a seventh calculation result to the processing block 20, and the processing block 20 converts the input signal by using the 32 bits from the 224 bit to the 255 bit of the extended key output from the extended key latch 22 as the parameter to output a converted signal. The exclusive OR of the output of the processing block 20 and the seventh calculation result of the above-described exclusive OR is calculated to output an eighth calculation result, and the eighth calculation result and the seventh calculation result as the significant 32 bits and the insignificant 32 bits are combined to output the scrambled text 14.

Further, another conventional data scrambling system has been proposed, as disclosed in Japanese Patent Laid-Open No. Sho 62-81145. In this case, input data are divided into a plurality of processing blocks, and the positional order configuration change of the processing blocks can be determined by both the input data and a scrambling key. However, in this case, it takes a long time to perform a descrambling.

As described above, in the conventional data scrambling systems, the address of the extended key input to each processing block from the extended key latch 22 is fixed, and hence an interceptor can readily analyze or decode the extended key in a communication path to which a chosen plaintext attack can be conducted.

Furthermore, as described above, in the conventional data scrambling systems, the order of the processing blocks is fixed, and thus the interceptor can analyze all of the extended key in the communication path to which the chosen plaintext attack can be conducted.

EP-A-0 406 457 discloses a method for the encoding/encryption and decoding/decryption of data, including partial stages and in which the key values for the individual partial stages are modified as a function of the data to be encoded with the aid of an electronic circuit. The key values necessary for decoding are obtained, without additional auxiliary values, from the data to be decoded. For this purpose in each partial stage of the method that part of the data which is used for producing the key value is not encoded and in each of the partial stages of the method another part of the data to be processed is used for producing key values.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide a data communication system and a method with a data scrambling improving random rate and security.

This object is solved by the features of the independent claims.

In these data communication system and method with a data scrambling, since the address of the cipher key or scramble function to be input to each processing block is varied depending on the input plaintext, the numbers of the usable cipher keys or scramble functions in one processing block is increased and a random rate of a cipher text becomes high and security is increased.

Further, since the order of the processing blocks depends on the plaintexts, a cipher sequence is varied each plaintext and thus the random rate of the cipher text becomes high.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects, features and advantages of the present invention will become more apparent from the consideration of the following detailed description, taken

in conjunction with the accompanying drawings, in which:

Fig. 1 is a schematic block diagram of a first embodiment of a data communication system with a data scrambling used in the present invention;
Fig. 2 is a schematic block diagram of a second embodiment of a data communication system with a data scrambling according to the present invention;
Fig. 3 is a schematic block diagram of a third embodiment of a data communication system with a data scrambling according to the present invention:
Fig. 4 is a schematic block diagram of a fourth embodiment of a data communication system with a data scrambling according to the present invention;
Fig. 5 is a schematic block diagram of a conventiona data scrambling system; and
Fig. 6 is a schematic block diagram of another conventional data scrambling system.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, wherein like reference characters designate like or corresponding parts throughout the views and thus the repeated description thereof can be omitted for brevioty, there is shown in Fig. 1 a first embodiment of a data communication system with a data scrambling which is used in the present invention.

As shown in Fig. 1, numerals 3 and 4 denote an 8 bytes of plaintext and an 8 bytes of scrambled text, respectively, and the data communication system with the data scrambling includes a plurality of processing blocks 9 to 16 for converting an input signal by using a part of extended keys as a parameter to output a converted data, a plurality of exclusive logical ORs 12, an address calculating circuit 23 for taking out addresses of the extended keys, a recording means such as a extended key latch 7 for storing a plurality of extended keys, two selectors 24 and 25 and a step counter 26. In this embodiment, the extended key latch 7, the address calculating circuit 23, the two selectors 24 and 25 and the step counter 26 constitute a selecting means 32 for selecting one of the extended keys.

Further, numerals 31, 32, 33 and 34 designate an input step for inputting data to be scrambled, a selecting means or step for selecting one of a plurality of extended keys, a scramble processing means or step for processing the scrambling of the input data, and an output step for outputting the scrambled data, respectively.

Next, the operation of the system shown in Fig. 1 will now be described in detail. At the initial state, the step counter 26 is set to "1", and the selectors 24 and 25 select the processing block 9. First, the input plaintext 3 is divided into more significant 4 bytes and less significant 4 bytes, and the less significant 4 bytes are input to the processing block 9 and the address calculating circuit 23 through the selector 24. The address calculating circuit 23 calculates an address of a extended key to be selected on the basis of the input plaintext data and outputs the calculated address to the extended key latch 7. The extended key latch 7 supplies the selected extended key corresponding to the given address to the selector 25, and the key is transmitted to the processing block 9 through the selector 25. The processing block 9 scrambles the input plaintext data by using the selected key of the selector 25 as the parameter and outputs a scrambled data. Then, in the exclusive OR 12, the output data of the processing block 9 and the more significant 4 bytes of the plaintext 3 are calculated, and the calculated result and less significant 4 bytes of the input plaintext data are replaced with each other to output to a next step.

Then, the step counter 26 counts up to set "2", and the selectors 24 and 25 are prepared to select the processing block 10. The less significant 4 bytes of the output of the first step are input to the processing block 10 and the address calculating circuit 23 through the selector 24. The address calculating circuit 23 calculates the address of the extended key to be selected on the basis of the input data and outputs the calculated address to the extended key latch 7. The extended key latch 7 supplies the selected extended key corresponding to the given address to the selector 25, and the key is transmitted to the second processing block 10 through the selector 25. The processing block 10 scrambles the input data by using the selected key of the selector 25 as the parameter and outputs a secondary scrambled data. Then, in the exclusive OR 12, the output data of the processing block 10 and the less significant 4 bytes of the plaintext data are calculated, and the calculated results of the two scramble processing means are replaced with each other to output to a next step.

Then, the same processing as described above is repeated predetermined times, and the more significant 4 bytes and the less significant 4 bytes of the scrambled data are replaced with each other to obtain the scrambled text 4 to be output.

In Fig. 2, there is shown the second embodiment of a data communication system with a data scrambling according to the present invention, having the same structure as the first embodiment shown in Fig. 1, except that a 2 bytes of scrambled text 4 is formed from a 2 bytes of plaintext 3 by using 4 steps of processing blocks 9 to 12 for making the explanation simple.

In this embodiment, a scramble function "f" for circularly shifting one bit to the left by adding is provided in each processing block 9, 10, 11 or 12. In this case, a cipher key is added to input data to be scrambled (a less significant 8 bits of the plaintext in the first step), and the MSB (most significant bit) of an addition result is circularly shifted to the LSB (least significant bit). Also, it is considered that in the extended key latch 7 (one example of the recording means), four cipher keys exhibited by a combination of hexadecimal 2 bits, such as, "FF",

"F0", "0F" and "C3" are recorded in respective addresses 0 to 3. In the method for selecting one of the four cipher keys, the less significant 2 bits of the input data to be scrambled (the part of the plaintext in the first step) are used as the address of the extended key latch.

The operation of the above-described system will now be described in detail when hexadecimal 2 bytes of data "00, 00" as the plaintext 3 are given under these conditions.

First, the plaintext "00, 00" is divided into a more significant 1 byte and a less significant 1 byte such as "00" and "00". The insignificant 1 byte "00" is input to the first scramble processing block 9 and the selecting means 32. Since the less significant 2 bits of "00" are 00, the selecting means 32 selects the address 0 and "FF" as the extended key. This key "FF" is input to the scramble processing block 9 through the selecting means 32. In the scramble processing block 9, by acting the scramble function f, the cipher key "FF" is added to the less significant 1 byte "00" to obtain 11111111 = "FF", and then the MSB of the obtained data is circularly shifted to the LBS to obtain a scrambled data 11111111 = "FF". As a result, the scramble processing block 9 outputs "FF" to a next step.

In the scramble processing block 10 of the second step, the output "FF" of the first scramble processing block 9 is input. Also, the cipher key "C3" at the address "3" of the extended key latch 7 is selected from the less significant 2 bits "11" of the previously scrambled result in the first scramble processing means and is input to the second scramble processing block 10 through the selecting means 32 In the scramble processing block 10, by acting the scramble function f, the cipher key "C3" is added to the input data "FF" to be scrambled to obtain 11000010, and then the MSB of the obtained data is circularly shifted to the LBS to obtain a scrambled data 10000101 = "85".

Then, the same processing as described above are repeated further two times at the third and fourth scramble processing means, and the scrambled text 4 of "8F, 15" is obtained and is output.

Although the above-described operation is performed for scrambling the input plaintext 3, when the scrambled text 4 is descrambled to the plaintext 3, same manner explained in the above operation can be used except to count down the counter backward.

As described above, according to the present invention, the scrambling system includes at least one scramble processing block which receives the cipher key as the parameter or the extended key output from the cipher key recording menas and performs the scrambling of the input data by using the parameter to output the scrambled data, and in one or more processing blocks, the selection of the cipher keys or the extended keys input to the scramble processing blocks is varied depending on the data to be scrambled such as the plaintext.

Further, although the cipher key is selected according to the input plaintext (or the input data to be scrambled) in the above-described embodiments, a plurality of scramble functions f can be stored and proper one of the scramble functions can be selected.

In Fig. 3, there is shown the third embodiment of a data communication system with a data scrambling according to the present invention, having the same structure as the first and second embodiments shown in Figs. 1 and 2, except that a plurality of scramble functions fn such as f_1 to f_4 are stored in the extended key latch 7. In this scramble function, a cipher key is added to input data to be scrambled, and the MSB of the obtained data is circularly shifted to the LSB by n times. In Fig. 3, corresponding parts to those shown in Fig. 2 denote corresponding numbers added by 100 and thus the detailed description thereof can be omitted for brevity.

In this embodiment, the operation of the system is carried out in the same manner as described above, except that not only the cipher key but also the scramble function fn are selected from the less significant 2 bits of the input data, and each processing block produces the scrambled data by using both the cipher key and the scramble function fn.

Although only cipher key is selected in the previous embodiments or both the cipher key and the scramble function are selected in this embodiment, only the scramble function can be selected according to the present invention.

In Fig. 4, there is shown the fourth embodiment of a data communication system with a data scrambling according to the present invention. As shown in Fig. 4, the system includes a loop counter 201, an input data selector 202 to receive 64 bits of an input plaintext 203, scramble processing means 204, 205 and 206 for scrambling an input data by using a extended keys as a parameter to output a scrambled data, a extended key latch 207 as a recording means for storing a plurality of extended keys, an output data selector 208 outputing 64 bits of scrambled text 214, scramble processing blocks 209, 210 and 211, exclusive logical ORs 212, and a cipher selecting means 232 having the same structure and function as the selecting means in the previous embodiments.

Further, numerals 251, 252 and 253 denote a processing step for producing a plurality of scrambled data in the scramble processing means 204, 205 and 206, a scrambled data selecting step for selecting one of a plurality of scrambled data produced in the scramble processing step 251, an output step for outputting the scrambled text 214, respectively.

Next, the operation of the system shown in Fig. 4 will now be described in detail. At the initial state, the loop counter 201 is set to "1", and the input data selector 202 selects the input plaintext 203. First, the 64 bits of input plaintext 203 passed through the input data selector 202 is divided into more significant 32 bits and less significant 32 bits. The more significant 32 bits are input to the three exclusive logical ORs 212 and the less sig-

nificant 32 bits are input to the scramble processing blocks 209, 210 and 211, the cipher selecting means 232 and the output data selector 208. The cipher selecting means 232 calculates an address of a extended key to be selected on the basis of the input 32 bits data and the output of the loop counter 201 by a predetermined method and selects the 32 bits of extended key present at the calculated address to output the selected extended key to all of the scramble processing blocks 209, 210 and 211. In this case, for example, regarding the address calculation method, the address can be determined from the less significant bits as described in the first embodiment, and any particular address calculating can be used.

In the scramble processing means 204, first, the input insignificant 32 bits and the 32 bits of extended key output from the cipher selecting means 232 are input to the scramble processing block 209 and the processing block 209 performs a scramble function transformation to the input data. In the exclusive OR 212, of the output of the processing block 209 and the more significant 32 bits of the plaintext 203 is calculated, and the calculation result and the less significant 32 bits of the input plaintext data are replaced with each other to output the first scrambled data to the output data selector 208. In the second scramble processing means 205, the same processing as that in the first scramble processing means 204 is performed by using the processing block 210 to output the second scrambled data to the output data selector 208. In the third scramble processing means 206, the same processing as that in the scramble processing means 204 is performed by using the processing block 211 to output the third scrambled data to the output data selector 208.

In the output data selector 208, by using the less significant 32 bits of the output of the input data selector 202, one of the outputs of the scramble processing means 204, 205 and 206 is selected and output at the scramble data selecting step 252.

As to which one of the outputs of the scramble processing means 204, 205 and 206 is selected, for example, the selection can be determined by using the less significant 2 bits of the less significant 32 bits as described in the first embodiment, and also by considering the less significant 32 bits as a numerical value, the selection can be performed by numbers (0, 1, 2) of remainders of a division by 3.

Next, the output of the output data selector 208 is input to the input data selector 202. The loop counter 201 counts up to "2", and the input data selector 202 selects the output of the output data selector 208.

Then, the same processing as described above is repeated predetermined times while the loop counter 201 counts up "1" at a time, and the output of the output data selector 208 is output as the scrambled text 214 to finish the operation at the output step 253.

Although the above-described operation is performed for scrambling the input plaintext, when the scrambled text is descrambled to the plaintext, by selecting the plain text only at the initial time and then the output of the output data selector 208 by the input data selector 202, same manner explained in the above operation can be used except to count down the loop counter 201 backward.

As described above, in this embodiment, the scrambling system includes at least two processing block which receive a part of the cipher key as the parameter or a part of the extended key output from the cipher key recording means and performs the scrambling of the input data by using the parameter to output the scrambled data, and the order of two or more of the processing blocks is varied depending on the plaintext or the data to be scrambled.

In the above-described embodiments, the description is carried out while the cipher key and the extended key are separated from each other, and according to the present invention, the cipher key is considered as the parameter for forming the cipher. Further, according to the present invention, the scramble function is considered as information directly or indirectly exhibiting a process for forming the cipher.

As described above, according to the present invention, since the content of the cipher key or the scramble function to be input to the processing block of each step can be varied depending on the content of the plaintext, high random rate can be obtained and thus the possibility of decoding or analysis of the data communication can be reduced.

Further, according to the present invention, since the selection of the extended keys can be performed depending on the content of the data to be scrambled such as the plaintext in the cipher selecting means, the content of each processing can be varied depending on the content of the data to be scrambled, and thus the high random rate can be obtained so as to reduce the possibility of decoding or analysis of the data communication.

Claims

1. A data communication system with a data scrambling of a bit array configureation of a digital data array of an input plaintext according to a predetermined conversion rule, comprising:

   scramble processing means (9-12; 109-112) for scrambling digital data by using a cipher key;
   recording means (7, 107) for storing a plurality of cipher keys;
   selecting means (32, 132) for selecting at least one cipher key from the recording means (7, 107) on the basis of at least a part of the input digital data to supply the selected cipher key to the scramble processing means (9-12,

109-112),

characterizing in that

said scramble processing (9-12, 109-112) means is storable with a scramble function and applies input digital data and the cipher key to the stored scramble function;
said recording means (7, 107) stores a plurality of scramble functions; and
said selecting means (32, 132) selects additionally one scramble function from the recording means and supplies the selected cipher key and the selected scramble function to the scramble processing means.

2. The system of claim 1,
characterized in that
a plurality of the scramble processing means (9-12, 102-112) are connected in series, and the selecting means (32, 132) selects a predetermined cipher key and the scramble function from the recording means (7, 107) on the basis of a part of output data of the scramble processing (9-12, 109-112) at a previous step and supply the selected cipher key and the selected scramble function to the scramble processing means at a next step.

3. The system of claim 2,
characterized by further comprising a step counter (26) for counting scrambling steps.

4. A data communication method with a data scrambling of a bit array configuration of a digital data array of an input plaintext according to a predetermined conversion rule, performing a scrambling processing by using the digital data and a cipher key,
characterized by the steps of:

selecting one of cipher keys and one of scramble functions on the basis of at least a part of the input digital data array; and
performing the scramble processing by applying input digital data and the selected cipher key to the selected scramble function.

5. The method of claim 4,
characterized in that
a plurality of the scramble processing means are connected in series, and the cipher key and the scramble function of the scramble processing on and after a second step is selected from a plurality of cipher keys and a plurality of scramble functions recorded by using a part of data of a scramble output at a previous step.

6. The method of claim 4, wherein the scramble processing is performed in the following steps:

dividing the input digital data array into significant bits and insignificant bits;
adding a cipher key to insignificant bits data of the input digital data array to obtain an addition result;
circularly shifting the most significant bit of the addition result to the least significant bit of the same n times to obtain a shift result; and
performing an exclusive OR of the shift result and significant bits data of the input digital data array to obtain a calculation result to output the calculation result as the insignificant bits data and the insignificant bits data of the input digital data array as the significant bits data.

7. A data communication system with a data scrambling of a bit array configuration of a digital data arrray of an input plaintext according to a predetermined conversion rule, comprising:

scramble processing means (9-12; 109-112) for scrambling digital data by using a cipher key;
recording means (7, 107) for storing a plurality of cipher keys;
selecting means (32, 132) for selecting at least one cipher key from the recording means (7, 107) on the basis of at least a part of the input digital data to supply the selected cipher key to the scramble processing means (9-12, 109-112),

characterized in that

a plurality of said scramble processing means (209-211) is connected in parallel, each scramble processing means storable with a scramble function for scrambling digital data by applying input digital data and a cipher key to the stored scramble function;
said cipher key selecting means (232) selects any one of the cipher key from the recording means (207) and supplies the selected cipher key to each scramble processing means (209-211); and
output selecting means (208) are provided for selecting any one of outputs of a plurality of the scramble processing means on the basis of at least the part of the input digital data.

8. The system of claim 7,
characterized by further comprising:

input selecting means (202) for selecting an output of either the input digital data array or the output selecting means (208) and supplying

the selected output to each scramble processing means (209-211); and
a loop counter (201) for counting scrambling times of each scramble processing means.

9. A data communication method with a data scrambling of a bit array configuration of a digital data array of an input plaintext according to a predetermined conversion rule, performing a scrambling processing by using the digital data and at least a cipher key;

characterized by comprising the steps of:

selecting one of cipher keys on the basis of a part of the input digital data array;
performing a plurality of scramble processings in parallel by using scramble functions individually given on the basis of input digital data and the selected cipher key; and
selecting any one of scramble outputs performed in parallel on the basis of at least a part of the input digital data.

10. The method of claim 9, wherein the performance of a plurality of the scramble processings in parallel is repeated plural times.

Patentansprüche

1. Datenkommunikationssystem mit einer Datenverwürfelung einer Bitanordnungs-Konfiguration einer digitalen Datenanordnung eines eingegebenen Klartextes gemäß einer vorbestimmten Umsetzungsregel, welches aufweist:

Würfelverarbeitungsmittel (9-12;109-112) zum Verwürfeln digitaler Daten durch Verwendung eines Ziffernschlüssels;
Aufzeichnungsmittel (7,107) zum Speichern mehrerer Ziffernschlüssel;
Auswahlmittel (32,132) zur Auswahl wenigstens eines Ziffernschlüssels aus den Aufzeichnungsmitteln (7,107) auf der Grundlage wenigstens eines Teils der eingegebenen digitalen Daten, um den ausgewählten Ziffernschlüssel zu den Würfelverarbeitungsmitteln (9-12,109-112) zu liefern,

dadurch gekennzeichnet, daß

die Würfelverarbeitungsmittel (9-12,109-112) mit einer Würfel funktion speicherbar sind und eingegebene digitale Daten und den Ziffernschlüssel auf die gespeicherte Würfel funktion anwendet;
die Aufzeichnungsmittel (7,107) mehrere Würfelfunktionen speichern;
und
die Auswahlmittel (32,132) zusätzlich eine Würfelfunktion aus den Aufzeichnungsmitteln auswählen und den ausgewählten Ziffernschlüssel und die ausgewählte Würfel funktion zu den Würfelverarbeitungsmitteln liefern.

2. System nach Anspruch 1, dadurch gekennzeichnet, daß
mehrere der Würfelverarbeitungsmittel (9-12, 102-112) in Reihe verbunden sind und die Auswahlmittel (32,132) einen vorbestimmten Ziffernschlüssel und die Würfelfunktion aus den Aufzeichnungsmitteln (7,107) auf der Grundlage eines Teils von Ausgangsdaten der Würfelverarbeitung (9-12,109-112) in einem vorhergehenden Schritt auswählen und in einem nächsten Schritt den ausgewählten Ziffernschlüssel und die ausgewählte Würfel funktion zu den Würfelverarbeitungsmitteln liefern.

3. System nach Anspruch 2, dadurch gekennzeichnet, daß weiterhin ein Schrittzähler (26) zum Zählen von Verwürfelungsschritten vorgesehen ist.

4. Datenkommunikationsverfahren mit einer Datenverwürfelung einer Bitanordnungs-Konfiguration einer digitalen Datenanordnung eines eingegebenen Klartextes gemäß einer vorbestimmten Umsetzungsregel, welches eine Verwürfelungsverarbeitung durch Verwendung der digitalen Daten und eines Ziffernschlüssels durchführt,
gekennzeichnet durch die Schritte:

Auswählen eines der Ziffernschlüssel und einer der Würfel funktionen auf der Grundlage wenigstens eines Teils der eingegebenen digitalen Datenanordnung; und
Durchführen der Verwürfelungsverarbeitung durch Anwenden eingegebener digitaler Daten und des ausgewählten Ziffernschlüssels auf die ausgewählte Würfel funktion.

5. Verfahren nach Anspruch 4, dadurch gekennzeichnet, daß
mehrere der Würfelverarbeitungsmittel in Reihe verbunden sind und der Ziffernschlüssel und die Würfelfunktion der Verwürfelungsverarbeitung auf einen und nach einem zweiten Schritt ausgewählt werden aus mehreren Ziffernschlüsseln und mehreren aufgezeichneten Würfelfunktionen durch Verwendung eines Teils von Daten eines Verwürfelungsausgangssignals bei einem vorhergehenden Schritt.

6. Verfahren nach Anspruch 4, worin die Verwürfelungsverarbeitung in den folgenden Schritten durchgeführt wird:

Teilen der eingegebenen digitalen Datenanordnung in bedeutende Bits und unbedeutende Bits;
Hinzufügen eines Ziffernschlüssels zu unbedeutenden Bitdaten der eingegebenen digitalen Datenanordnung, um ein Summenergebnis zu erhalten;
n-faches kreisförmiges Verschieben des bedeutendsten Bits des Summenergebnisses zu dem unbedeutendsten Bit desselben, um ein Verschiebungsergebnis zu erhalten;
und
Durchführen einer EXKLUSIV-ODER-Funktion bei dem Verschiebungsergebnis und bedeutenden Bitdaten der eingegebenen digitalen Datenanordnung, um ein Berechnungsergebnis zu erhalten, zur Ausgabe des Berechnungsergebnisses als die unbedeutenden Bitdaten und der unbedeutenden Bitdaten der eingegebenen digitalen Datenanordnung als die bedeutenden Bitdaten.

7. Datenkommunikationssystem mit einer Datenverwürfelung einer Bitanordnungskonfiguration einer digitalen Datenanordnung eines eingegebenen Klartextes gemäß einer vorbestimmten Umsetzungsregel, welches aufweist:

Würfelverarbeitungsmittel (9-12;109-112) zum Verwürfeln digitaler Daten durch Verwendung eines Ziffernschlüssels;
Aufzeichnungsmittel (7,107) zum Speichern mehrerer Ziffernschlüssel;
Auswahlmittel (32,132) zur Auswahl wenigstens eines Ziffernschlüssels aus den Aufzeichnungsmitteln (7,107) auf der Grundlage wenigstens eines Teils der eingegebenen digitalen Daten, um den ausgewählten Ziffernschlüssel zu den Würfelverarbeitungsmitteln (9-12,109-112) zu liefern,

dadurch gekennzeichnet, daß

mehrere der Würfelverarbeitungsmittel (209-211) parallel verbunden sind, wobei jedes der Würfelverarbeitungsmittel speicherbar ist mit einer Würfelfunktion zum Verwürfeln digitaler Daten durch Anwenden eingegebener digitaler Daten und eines Ziffernschlüssels auf die gespeicherte Würfel funktion;
die Ziffernschlüssel-Auswahlmittel (232) irgendeinen der Ziffernschlüssel aus den Speichermitteln (207) auswählen und den ausgewählten Ziffernschlüssel zu jedem der Würfelverarbeitungsmittel (209-211) liefern; und
Ausgangssignal-Auswahlmittel (208) vorgesehen sind zur Auswahl irgendeines von Ausgangssignalen von mehreren der Würfelverarbeitungsmittel auf der Grundlage wenigstens des Teils der eingegebenen digitalen Daten.

8. System nach Anspruch 7, weiterhin gekennzeichnet durch
Eingangssignal-Auswahlmittel (202) zur Auswahl eines Ausgangssignals von entweder der eingegebenen digitalen Datenanordnung oder den Ausgangssignal-Auswahlmitteln (208) und zum Liefern des ausgewählten Ausgangssignals zu jedem Würfelverarbeitungsmittel.

9. Datenkommunikationsverfahren mit einer Datenverwürfelung einer Bitanordnungs-Konfiguration einer digitalen Datenanordnung eines eingegebenen Klartextes gemäß einer vorbestimmten Umsetzungsregel, welches eine Verwürfelungsverarbeitung durch Verwendung der digitalen Daten und wenigstens eines Ziffernschlüssels durchführt, **gekennzeichnet** durch die Schritte:

Auswahl eines der Ziffernschlüssel auf der Grundlage eines Teils der eingegebenen digitalen Datenanordnung;
paralleles Durchführen mehrerer Verwürfelungsverarbeitungen durch Verwenden von Würfelfunktionen, die individuell auf der Grundlage von eingegebenen digitalen Daten und des ausgewählten Ziffernschlüssels gegeben sind; und
Auswählen irgendeines von parallel durchgeführten Verwürfelungs-Ausgangssignalen auf der Grundlage wenigstens eines Teils der eingegebenen digitalen Daten.

10. Verfahren nach Anspruch 1, worin die parallele Durchführung mehrerer der Verwürfelungsverarbeitungen mehrere Male wiederholt wird.

Revendications

1. Système de communication de données présentant un brouillage de données d'une configuration binaire d'un réseau de données numériques d'un texte en clair d'entrée selon une règle de conversion prédéterminée, comprenant :

des moyens de traitement de brouillage (9-12; 109-112) pour brouiller des données numériques en utilisant une clé chiffrée,
des moyens d'enregistrement (7, 107) pour stocker une série de clés chiffrées,
des moyens de sélection (32, 132) pour sélectionner au moins une clé chiffrée des moyens d'enregistrement (7, 107) sur la base d'au moins une partie des données numériques d'entrée pour délivrer la clé chiffrée sélection-

née aux moyens de traitement de brouillage (9-12; 109-112),

caractérisé en ce que :

lesdits moyens de traitement de brouillage (9-12; 109-112) peuvent être stockés avec une fonction de brouillage et appliquent des données numériques d'entrée et la clé chiffrée à la fonction de brouillage stockée,
lesdits moyens d'enregistrement (7, 107) stockent une série de fonctions de brouillage; et
lesdits moyens de sélection (32, 132) sélectionnent en outre une fonction de brouillage dans les moyens d'enregistrement et délivrent la clé chiffrée sélectionnée et la fonction de brouillage sélectionnée aux moyens de traitement de brouillage.

2. Système selon la revendication 1, caractérisé en ce que :
une série des moyens de traitement de brouillage (9-12; 102-112) sont connectés en série et les moyens de sélection (32, 132) sélectionnent une clé chiffrée prédéterminée et la fonction de brouillage dans les moyens d'enregistrement (7, 107) sur la base d'une partie des données de sortie des moyens de traitement de brouillage (9-12; 109-112) d'une étape précédente et délivrent la clé chiffrée sélectionnée et la fonction de brouillage sélectionnée aux moyens de traitement de brouillage de l'étape suivante.

3. Système selon la revendication 2, caractérisé en ce qu'il comprend par ailleurs un compteur d'étapes (26) pour compter les étapes de brouillage.

4. Procédé de communication de données présentant un brouillage de données d'une configuration binaire d'un réseau de données numériques d'un texte en clair d'entrée selon une règle de conversion prédéterminée, pour effectuer un traitement de brouillage en utilisant les données numériques et une clé chiffrée, caractérisé par les étapes suivantes :

on sélectionne l'une des clés chiffrées et l'une des fonctions de brouillage sur la base d'au moins une partie du réseau de données numériques d'entrée, et
on effectue le traitement de brouillage en appliquant des données numériques d'entrée et la clé chiffrée sélectionnée à la fonction de brouillage sélectionnée.

5. Procédé selon la revendication 4, caractérisé en ce que :
une série des moyens de traitement de brouillage sont connectés en série et la clé chiffrée et la fonction de brouillage des moyens de traitement de brouillage au cours d'une deuxième étape et après celle-ci sont sélectionnées parmi une série de clés chiffrées et une série de fonctions de brouillage enregistrées en utilisant une partie des données d'une sortie de brouillage dans une étape précédente.

6. Procédé selon la revendication 4, dans lequel le traitement de brouillage est réalisé au cours des étapes suivantes :

on divise le réseau de données numériques d'entrée en bits significatifs et bits non significatifs,
on ajoute une clé chiffrée aux données de bits non significatifs du réseau de données numériques d'entrée pour obtenir un résultat par addition,
on décale par voie circulaire le bit le plus significatif du résultat de l'addition au bit le moins significatif de celle-ci n fois pour obtenir un résultat décalé, et
on effectue une combinaison exclusive OU du résultat du décalage et des données de bits significatifs du réseau de données numériques d'entrée pour obtenir un résultat de calcul afin de délivrer le résultat du calcul sous la forme des données de bits non significatifs et les données de bits non significatifs du réseau de données numériques d'entrée comme données de bits significatifs.

7. Système de communication de données présentant un brouillage de données d'une configuration binaire d'un réseau de données numériques d'un texte en clair d'entrée selon une règle de conversion prédéterminée, comprenant :

des moyens de traitement de brouillage (9-12; 109-112) pour brouiller des données numériques en utilisant une clé chiffrée,
des moyens d'enregistrement (7, 107) pour stocker une série de clés chiffrées,
des moyens de sélection (32, 132) pour sélectionner au moins une clé chiffrée dans les moyens d'enregistrement (7, 107) sur la base d'au moins une partie des données numériques d'entrée pour délivrer la clé chiffrée sélectionnée aux moyens de traitement de brouillage (9-12; 109-112),

caractérisé en ce que :

une série desdits moyens de traitement de brouillage (209-211) sont connectés en paral-

[à la cheveux moyen de traitement d'abrasivage

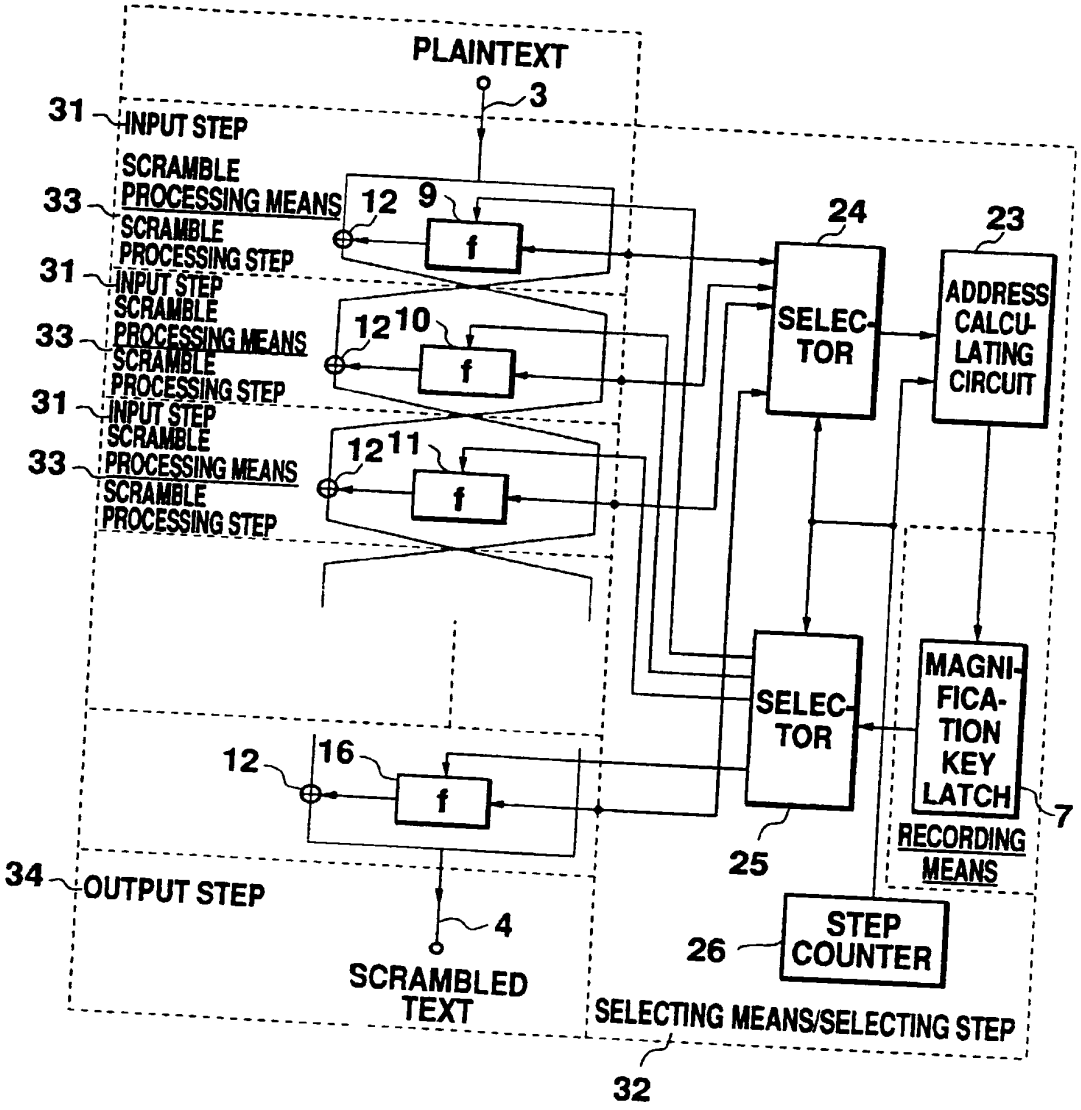
PLAINTEXT
3
31
INPUT STEP
SCRAMBLE PROCESSING MEANS
33
SCRAMBLE PROCESSING STEP
12
9
f
24
23
SELEC-TOR
ADDRESS CALCU-LATING CIRCUIT
31
INPUT STEP
SCRAMBLE PROCESSING MEANS
33
SCRAMBLE PROCESSING STEP
12
10
f
31
INPUT STEP
SCRAMBLE PROCESSING MEANS
33
SCRAMBLE PROCESSING STEP
12
11
f
SELEC-TOR
MAGNI-FICA-TION KEY LATCH
7
RECORDING MEANS
12
16
f
25
34
OUTPUT STEP
4
SCRAMBLED TEXT
26
STEP COUNTER
SELECTING MEANS/SELECTING STEP
32

Fig. 1

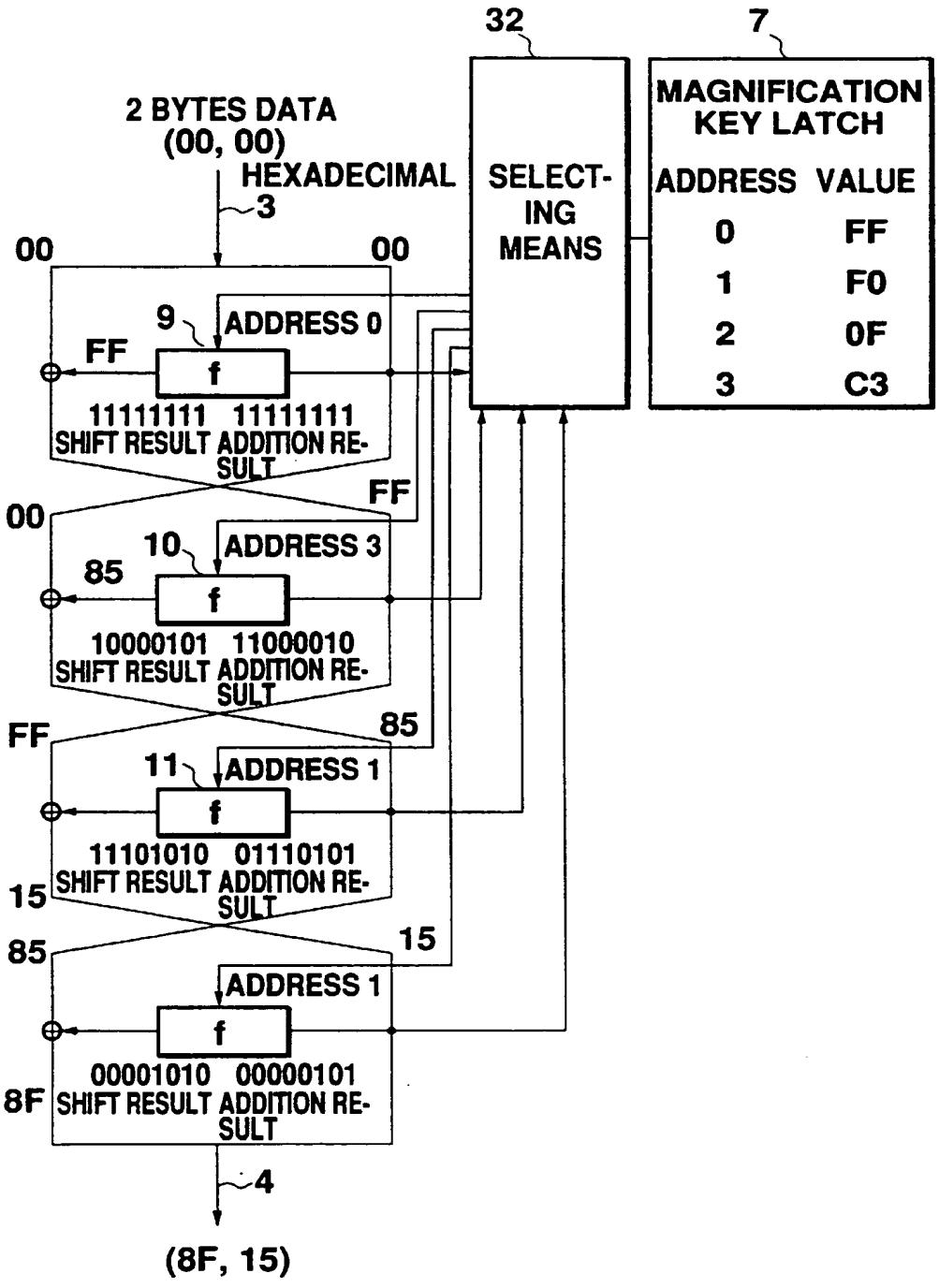
32
7
2 BYTES DATA
(00, 00)
HEXADECIMAL
3
SELECT-
ING
MEANS
MAGNIFICATION
KEY LATCH
ADDRESS VALUE
0 FF
1 F0
2 0F
3 C3
00
00
9
ADDRESS 0
FF
f
11111111 11111111
SHIFT RESULT ADDITION RE-
SULT
FF
00
10
ADDRESS 3
85
f
10000101 11000010
SHIFT RESULT ADDITION RE-
SULT
85
FF
11
ADDRESS 1
f
11101010 01110101
SHIFT RESULT ADDITION RE-
SULT
15
15
85
ADDRESS 1
f
00001010 00000101
8F SHIFT RESULT ADDITION RE-
SULT
4
(8F, 15)

Fig. 2

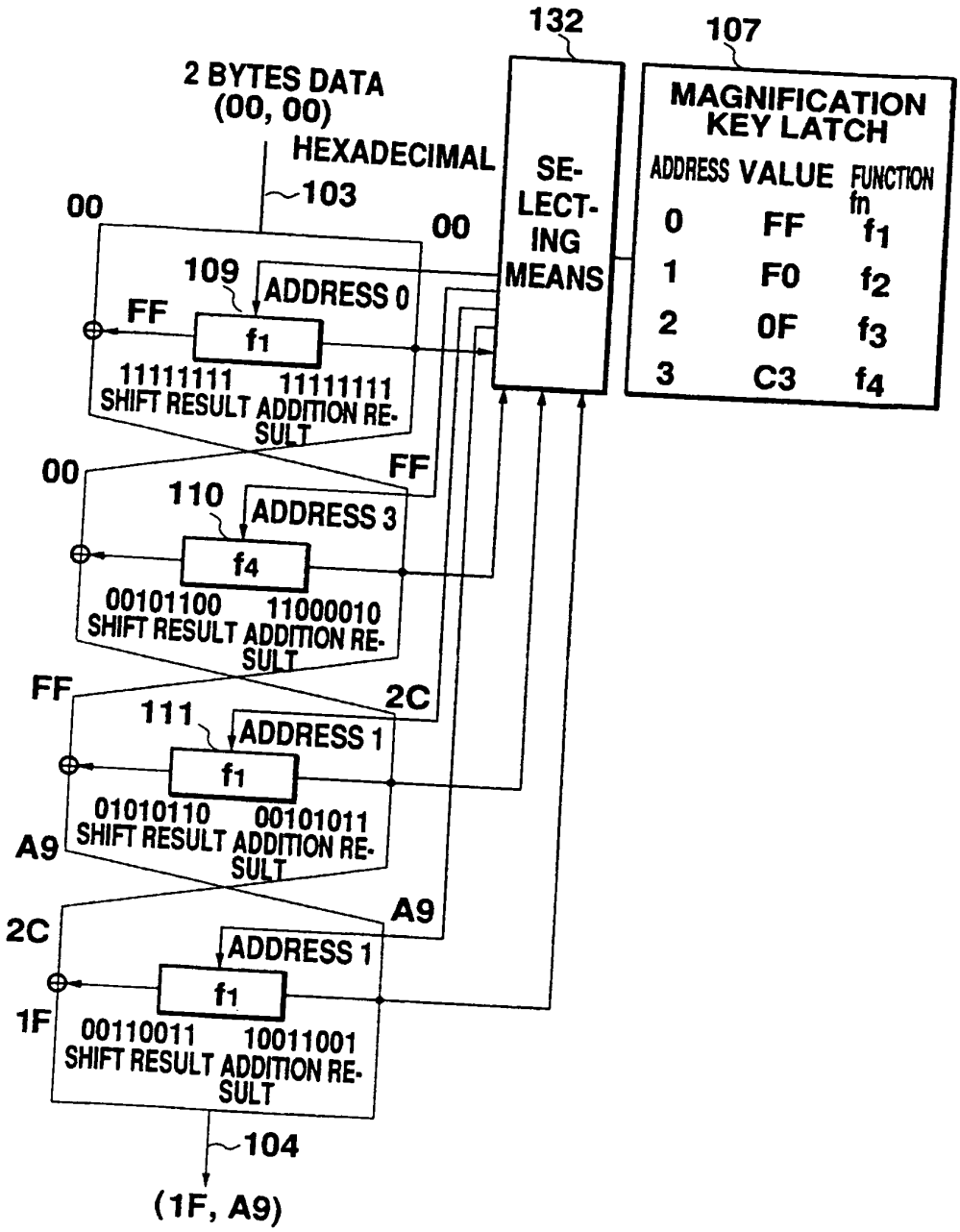
132
107
2 BYTES DATA
(00, 00)
HEXADECIMAL
103
SE-
LECT-
ING
MEANS
MAGNIFICATION
KEY LATCH
ADDRESS VALUE FUNCTION fn
0 FF f1
1 F0 f2
2 0F f3
3 C3 f4
00
00
109
ADDRESS 0
FF
f1
11111111 11111111
SHIFT RESULT ADDITION RE-
SULT
00
FF
110
ADDRESS 3
f4
00101100 11000010
SHIFT RESULT ADDITION RE-
SULT
FF
2C
111
ADDRESS 1
f1
01010110 00101011
SHIFT RESULT ADDITION RE-
SULT
A9
A9
2C
ADDRESS 1
f1
1F
00110011 10011001
SHIFT RESULT ADDITION RE-
SULT
104
(1F, A9)

Fig. 3

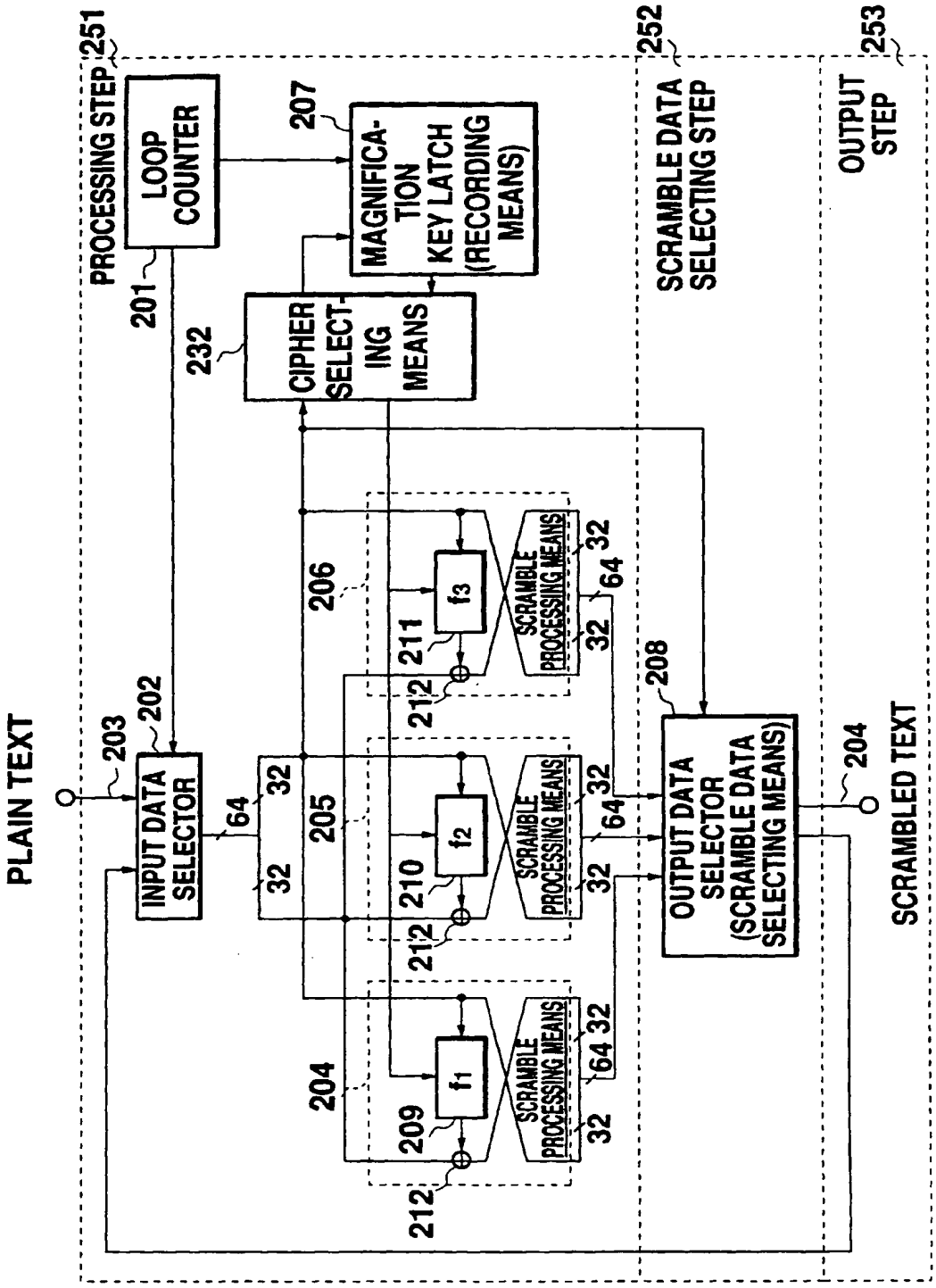
PLAIN TEXT
PROCESSING STEP
251
LOOP COUNTER
201
207
MAGNIFICA-TION KEY LATCH (RECORDING MEANS)
232
CIPHER SELECT-ING MEANS
SCRAMBLE DATA SELECTING STEP
252
OUTPUT STEP
253
203
202
INPUT DATA SELECTOR
64
32
32
205
206
204
f3
f2
f1
211
210
209
212
212
212
SCRAMBLE PROCESSING MEANS
32
64
32
208
OUTPUT DATA SELECTOR (SCRAMBLE DATA SELECTING MEANS)
204
SCRAMBLED TEXT

Fig. 4

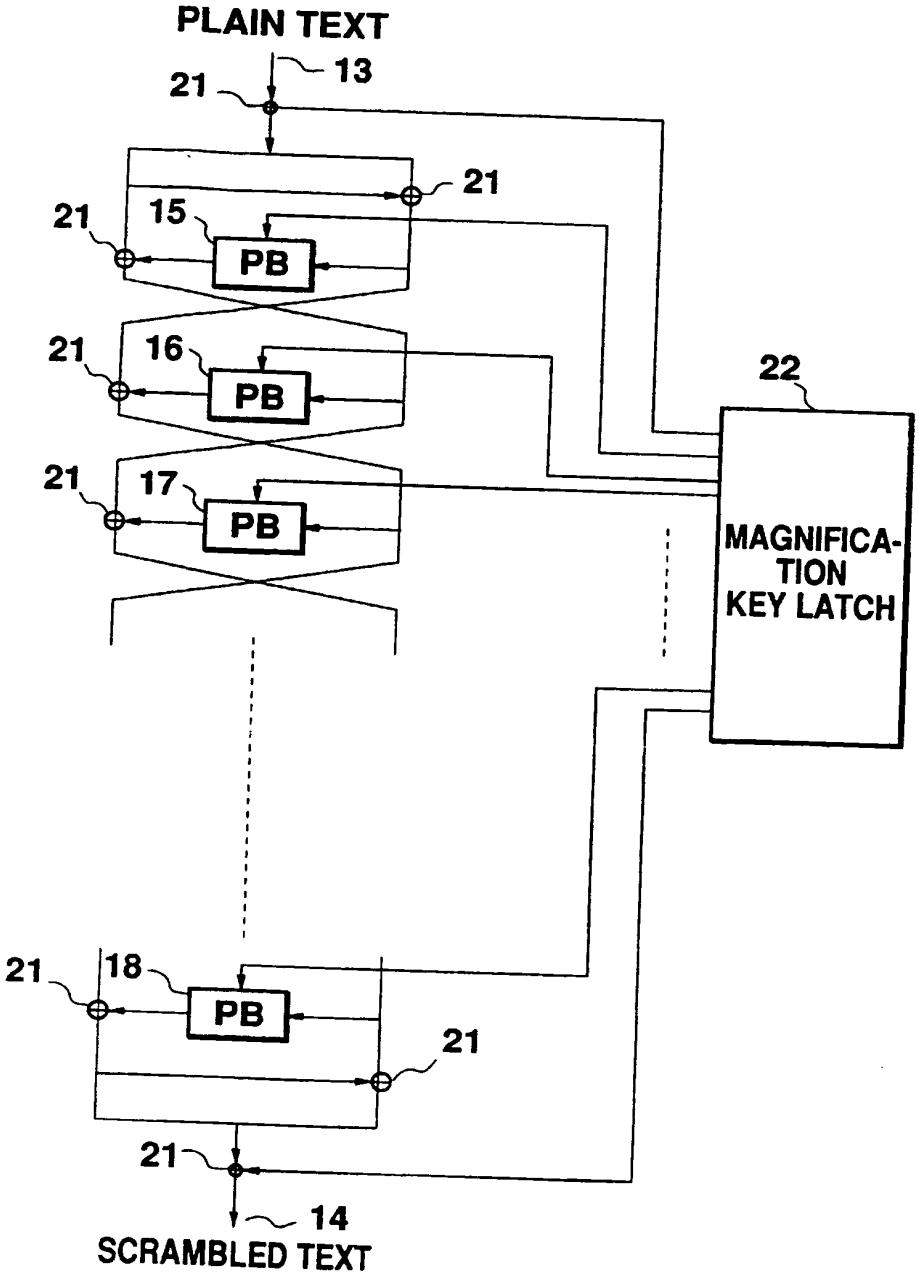
PLAIN TEXT
13
21
21
21
15
PB
21
16
PB
21
17
PB
22
MAGNIFICA-
TION
KEY LATCH
21
18
PB
21
21
14
SCRAMBLED TEXT

Fig. 5

PLAIN TEXT